SmartBox Security

Keycafe Security Architecture Overview

Introduction

Keycafe provides a convenient way for businesses to remotely manage keys while maintaining an acceptable security level for most use cases. From product design to systems architecture to solid SmartBox construction, our solutions are designed from the ground up with a balance of security, convenience and usability in mind. This overview describes the essential security features built into the Keycafe Smart Key Management platform.

Best-In-Class Server, Application & Database Architecture

State-of-the-art service & security

Keycafe integrates with best-in-class software providers to offer top level security on the back end. Transport Layer Security, Denial of Service attack protection, and Managed Firewalls are integral to our data server architecture. Keycafe observes security best practices such as password hashes, access logging, source code reviews and penetration testing.

Transport Layer Security

TLS encrypts, authenticates, and verifies data integrity against tampering. A private communication channel between your computer and Keycafe ensures that when you manage your account, all information is safely transmitted.

Denial of Service

Access to Keycafe is secured against Denial of Service (DDOS) attacks by a best-in-class CDN partner. With over 67 Tbps of network capacity, Cloudflare blocks an average of 70B threats per day to protect you against the largest and most sophisticated attacks.

Managed Firewalls

Your data is secure behind multiple state-of-the-art firewalls. Firewalls are fundamental to protecting network traffic including the flow of sensitive data. They are required for compliance to mandates like PCI DSS, HIPAA, and GDPR.

PCI Compliant Payment Processing

Your payment information is encrypted by a PCI compliant payment processor certified to PCI Service Provider Level 1, the most stringent level of certification available in the payments industry.

Penetration Testing

Keycafe periodically performs automated penetration testing to find vulnerabilities before they can be exploited. These tests, designed by security experts, simulate the activities of real hackers to flag issues like misconfigured servers, SQL injection, cross-site scripting, exposed files/directories, weak encryption protocols or cyphers, and many others. They also test for known vulnerabilities in popular software and protocols ("Heartbleed", etc.).

Our software suppliers equip Keycafe with constant, industry leading threat monitoring and automatic OS vulnerability patching. Selected Keycafe software providers include:

Cloudflare

World leader in DDoS protection, rate limiting, proxy for CDN performance improvements, and DNS management. Cloudflare is trusted by 25M internet properties.

Heroku

Highly advanced security for web hosting, systems administration, Linux security updates, database security updates, firewall, and software intrusion detection. Heroku is ISO 27001, 27017, 27108 compliant with SOC 1, 2, 3 reporting. **See more.**

Intruder.io

Intruder is a cloud-based vulnerability scanner that finds cyber security weaknesses in digital infrastructure by scanning for 10,000 common attack vectors.

Particle

Industry leading provider of IoT at scale enables the management of a highly secure network of remote devices, hardware, and cloud services.

Stripe

The leading online billing platform. Millions of businesses of all sizes—from startups to large enterprises—use Stripe's PCI compliant software and APIs to accept payments, send payouts, and manage their businesses online.

Keycafe scored an A+ with 99.98% security effectiveness score on an Intruder.io scan of over 10,000 attack vectors.

User Authentications & Permissions

Tailored access authentication

Keycafe user authentication offers a number of options to give you control over who accesses your business's key to rental properties, vehicles, and company facilities. As a default setting, two factor authentication is enabled requiring end users to input an ID number plus an access code sent via SMS message.

Depending on your subscription plan, a variety of additional custom permissions can be layered in for authentication, such administrative controls, scheduled permissions, badge scans, and more. Utilizing the full breadth of our user-facing authentication options and tailoring access to each user of your SmartBoxes is an important deterrent to unauthorized access to keys.

Below is a table of the types of objects that can be accessed and the permissions options that can be granted and managed.

Object / Permission Type	Description	Who Can Access	Authentication Requirement
Key Codes	A simple code that can be created for any key which when entered at the SmartBox, reveals the key. The key code is valid until withdrawn.	Any person you give the key code to	Inputting the key code on the SmartBox
Scheduled Bookings	An access to a key that is valid within a specific time frame where the party is not required to be a registered user.	Any person you give the booking details to	Entering the booking code at the SmartBox or utilizing the unique URL for the mobile friendly experience.
Single Key Permission	A permission in the database for a user or group of users to access a specific key.	Any user given exchange or admin permissions to the key, or any user in a group of users that has exchange or admin permissions to the key	Using Keycafe iOS or Android App, or entering ID code at SmartBox plus 2FA code if required by settings
All Keys Permission	A permission in the database for a user or group of users to access all keys owned by your account.	Any user given exchange or admin permissions to the all keys group, or any user in a group of users that has exchange or admin permissions to the all keys group	Using Keycafe iOS or Android App, or entering ID code at SmartBox plus 2FA code if required by settings.
Custom Group of Keys	A permission in the database for a user or group of users to access a group of keys you have designated.	Any user given exchange permissions, User given admin permissions to the custom key group, group of users with exchange or admin permissions to the custom key group	Using Keycafe iOS or Android App, or entering ID code at SmartBox plus 2FA code if required by settings.
Key Bin	An ability for a user to remotely open any key bin on the SmartBox regardless of key permissions.	Any user given admin permissions to the key exchange location	Using Keycafe web app, iOS or Android App.
SmartBox Main Lock	An ability for a user to remotely unlock from the wall the entire SmartBox regardless of key permissions	Any user given admin permissions to the key exchange location	Using Keycafe web app, iOS or Android App.

IoT Server to SmartBox Communication

Robust, dynamic & informative

By integrating with Particle's Device Cloud, Keycafe IoT security is backed by best-in-class hosting with ISO 27001, 27017, and 27018 physical security and risk management which minimizes attack surface area in both the service layer and data.

Advanced IoT Security

All communication between the SmartBox and our servers is encrypted and secure. Leaving no incoming ports open, our service thwarts port scanners and side attacks. Each device carries a unique encryption key, and continuous security landscape monitoring protects servers from potential threats.

Encrypted Radio Connections

BLE communication with the SmartBox is fully encrypted in transit. WiFi connections are secured using WPA2, the industry standard. Cellular connections use industry standard encryption to ensure all data is safe in transit.

Device Activity Alerts

With 24/7 SmartBox cloud connectivity, key exchanges automatically trigger detailed notifications in real time via email, mobile notifications, or webhook. Since authentication occurs live in communication with our server, Keycafe provides real-time control over access to your keys.

OTA Updates

Each SmartBox receives over the air updates which means firmware and security features are always up to date to stay one step ahead of emerging threats.

Sensitive Data Offsite

No sensitive data is stored locally on the Keycafe SmartBox. Meanwhile, encryption protocols add another critical layer of protection.

Privacy Policy & Data Processing

GDPR compliant

The Keycafe customer focused Privacy Policy outlines what information is collected and how it is used, shared, secured, and stored. Keycafe is headquartered in Vancouver, Canada and customer data is not processed on premises. We rely upon best in class third-party cloud service providers to process and store your information on our behalf and these providers may process and store your information in the United States, Canada, the European Union and other countries. We have verified these providers have GDPR compliance programs in place and have entered into data processing agreements with our service providers that restrict and regulate their processing of your data on our behalf.

Our systems contain rules and safeguards pertaining to what data is shown to other users depending on their permissions and the implied relationship between the parties. Additionally, we go beyond typical internal controls by not displaying user PII by default to our own team members and limiting the number of PII views each team member is allowed without reauthentication. You can access our complete Privacy Policy **here**.

The SmartBox

Solid deterrent from most tampering

Our steel plate mounted SmartBox features a rugged 16 gauge powder-coated steel frame. Inside, each individual key bin is constructed with a separate die cast metal enclosure. The electronic master lock is inaccessible and fully hidden from view. The SmartBox should deter most casual tampering by unauthorized parties given its solid metal construction, locks on each individual key bin, and lack of any externally facing master lock.

The Keycafe SmartBox is designed to have a security level similar to, for example, lockers at a train station or bike locks used in the city. It is not designed to resist burglars equipped with tools. It is worth noting that safes which have official anti- theft certifications for safeguarding valuables measure their hardness in the number of minutes they can resist a theft, typically 10 minutes or less, so even the most secure safes will in practice resist a party with malicious intent only for a limited period of time. Our product is not a safe or vault and is designed to provide usability and convenience coupled with solid construction. The SmartBox should only be used in well lit, surveilled environments you believe unlikely to attract theft. You should check with your insurance provider concerning how use and placement of the SmartBox may impact any claims.

SmartBox Features:

- 15-screw steel plate mount
- Sturdy 16 gauge cold rolled steel frame
- A383 alloy die cast metal key bins
- Inaccessible, electronically controlled master access
- Weather resistant powder coating

Each SmartBox is further protected by state-of-the-art IoT security, tailored authentication, and best-in-class software integrations as described above.

Further Information

While our support and sales teams do their best to communicate on a broad array of technical topics related to our products, their answers may not always be fully nuanced or up to date. This document provides a high level summary of our security architecture, practices and key vendors. If you have a security question not addressed by this document and require a definitive answer, please reach out to **security@keycafe.com** and we will consult our product leaders and engineers to provide you with additional information.